Goddard Procedural Requirements (GPR)

DIRECTIVE NO.	GPR 1600.1A	**APPROVED BY Signature:**	***Original Signed By***
EFFECTIVE DATE:	February 21, 2014	**NAME:**	Raymond Rubilotta
EXPIRATION DATE:	February 21, 2019	**TITLE:**	Director, Management Operations Directorate

COMPLIANCE IS MANDATORY

Responsible Office: Code 240/Goddard Space Flight Center Security Division

Title: Goddard Space Flight Center (GSFC) Protective Services Program Requirements

TABLE OF CONTENTS

PREFACE

P.1 PURPOSE

This directive establishes protective services procedures and requirements for the Goddard Space Flight Center (GSFC) and its component facilities as required in NASA Policy Directive (NPD) 1600.2E and NASA Procedural Requirements (NPR) 1600.1A. It establishes security program standards and requirements necessary to achieve Center-wide security program consistency and uniformity, while allowing reasonable flexibility in implementing risk management principles, where appropriate, at all GSFC facilities. It also describes management security responsibilities.

To ensure that all security requirements are met with minimum disruption to normal activities, this document defines the responsibilities, coordination, and controls to be followed. It describes both routine and emergency operations.

This directive implements the requirements of NPR 1600.1A at GSFC, and is organized such that it follows, chapter-by-chapter, the organization of the NPR.

P.2 APPLICABILITY

a. This GPR is applicable to all GSFC facilities, including component facilities, which in the context of this directive includes the Greenbelt site, the Wallops Flight Facility (WFF), the Goddard Institute for Space Studies (GISS), and the Independent Verification and Validation (IV&V) Facility. Exceptions or special provisions for specific sites are identified in the body of the document.

b. This GPR is applicable to all GSFC civil service employees, GSFC contractor employees, personnel completing work through Space Act Agreements, Memorandum of Agreement (MOA), or Memorandum of Understanding (MOU), those assigned or detailed under the Intergovernmental Personnel Act, partners, recipients of grants and cooperative agreements, and visitors.

c. In this directive all document citations are the latest version unless otherwise noted.

d. In this GPR all mandatory actions (i.e., requirements) are denoted by statements containing the term "shall." The terms: "may" or "can" denote discretionary privilege or permission, "should" denotes a good practice and is recommended, but not required, "will" denotes expected outcome, and "are/is" denotes descriptive materials.

P.3 AUTHORITIES

a. National Aeronautics and Space Act, as amended, 51 U.S.C. § 20113 (a)
b. NPR 1600.1A, NASA Security Program Procedural Requirements, August 12, 2013
c. NPD 1600.2E, NASA Security Policy

P.4 APPLICABLE DOCUMENTS AND FORMS

a. Violation of Regulations of National Aeronautics and Space Administration, 18 U.S.C. § 799.
b. Unlawful Acts, 18 U.S.C. § 922 (d) (9).
c. Atomic Energy Act of 1954, as amended, 42 U.S.C. § 2011 et seq.
d. Permission to Use Firearms, 51 U.S.C. § 20133.
e. Arrest Authority, 51 U.S.C. § 20134.
f. The Homeland Security Act, Pub. L. No. 107-296, 116 Stat. 2135 (2002).
g. Classified National Security Information, Exec. Order No. 13526, 75 C.F.R. 707 (2010).
h. Controlled Unclassified Information, Exec. Order No. 13556.
i. Chemical Facility Antiterrorism Standards (CFATS), 6 C.F.R. Part 27.
j. Security Programs; Arrest Authority and Use of Force by NASA Security Force Personnel, 14 C.F.R Part 1203(b).
k. Inspection of Persons and Personal Effects at NASA Installations or on NASA Property; Trespass or Unauthorized Introduction of Weapons or Dangerous Materials, 14 C.F.R. Part 1204, subpart 10.
l. NPD 1000.3D, NASA Organization (w/change 37, dated June 11, 2013).
m. NPR 1382.1, NASA Privacy Procedural Requirements.
n. NPD 1440.6H, NASA Records Management.
o. NPD 1600.3, NASA Prevention of and Response to Workplace Violence.
p. NPD 1600.4, National Security Programs.
q. NPR 1600.2, NASA Classified National Security Information (CNSI).
r. NPR 1600.3, NASA Personnel Security.
s. NPR 1620.2, Facility Security Assessments.
t. NPR 1620.3A, Physical Security Requirements for NASA Facilities and Property.
u. NPR 2810.1, Security of Information Technology.
v NPR 4200.1, NASA Equipment Management Procedural Requirements.
w. NPR 8000.4A, Agency Risk Management Procedural Requirements.
x. NPR 8621.1, NASA Procedural Requirements for Mishap and Close Call Reporting, Investigating, and Recordkeeping (w/Change 6, dated October 24, 2011).
y. NPR 8715.3, NASA General Safety Program Requirements (w/Change 8 dated June 20, 2012).
z. NPR 8621.1, NASA Procedural Requirements for Mishap and Close Call Reporting, Investigating,

and Recordkeeping (w/Change 6, dated October 24, 2011).
aa. NPR 8715.3, NASA General Safety Program Requirements (w/Change 8 dated June 20, 2012).
bb. NASA Technical Standard (NASA-STD) 8719.12, Safety Standard for Explosives, Propellants, and Pyrotechnics.
cc. GSFC Form 24-10D, Lost/Missing/Stolen Property Report
dd. GSFC Form 24-12, Key Request/Receipt Form
ee. GSFC Form 24-12A, Keycard Request/Receipt Form
ff. GSFC Form 24-27, Locator and Information Services Tracking System (LISTS) Data
gg. NASA Technical Standard (NASA-STD) 8719.12, Safety Standard for Explosives, Propellants, and Pyrotechnics.
hh. Sensitive Compartmented Information Facilities (SCIFs), Director of National Intelligence (DNI) Intelligence Community Directive (ICD) 705.
ii. Technical Surveillance Countermeasures (TSCM) ICD 702.
jj. NSDD 298: National Operations Security Program.
kk. Critical Infrastructure Security and Resilience Presidential Policy Directive (PPD)-21.
ll. Homeland Security - Interagency Security Committee Standards (ISC), Physical Security Criteria for Federal Facilities (2010).

P.5 CANCELLATION

GPR 1600.1, Goddard Security Requirements

P.6 SAFETY

None

P.7 TRAINING

a. All GSFC civil service employees and contractors shall take all required training and attend all briefings identified in paragraph 2.19.2 of this GPR; and
b. All GSFC civil service employees, contractors, tenants and others shall take all required training from the System for Administration, Training, and Educational Resources for NASA (SATERN); and
c. The Goddard Protective Services Division (GPSD) shall administer annual Federal Arrest Authority (FAA) and Use of Force training to security personnel as described in NPR 1600.1A, Chapter 6.

P.8 RECORDS

The table below lists both the records required by this GPR and those required by NPR 1600.1A. See Appendix 2 for identification of acronyms. The term “appropriate” in the Record Custodian column means the location appropriate for a given GSFC site, e.g., the Greenbelt GPSD Office as opposed to the Wallops GPSD Office, GISS, and IV&V.

No.	Record Title	Record Custodian	Retention
2	Key Accountability Files – Under Maximum Security	Appropriate GPSD key control office	*NRRS 1/99A Destroy 3 years after turn in of key.
3	Key Accountability Files – All Other Areas	Appropriate GPSD key control office	*NRRS 1/99B Destroy 6 months after turn in of key.
4	Contractor Security Officer Assignment Files	Appropriate security office	*NRRS 1/100A Destroy 3 years after final entry.
5	Contractor Security Officer Control Files	Appropriate security office	*NRRS 1/100B Destroy when superseded or obsolete.
12	GSFC LISTS database – NASA 51 LIST (GSFC Form 24-27)	GPSD LISTS Manager	*NRRS 1/104 Records are retained for varying periods of time, in compliance with NPR 1441.1 and the Privacy Act System Notice. Contact the Center Records Manager.
13	Identification Credentials Files, including cards, badges, parking permits, photographs, agency permits to operate motor vehicles, and property, cafeteria(s), and visitor passes, and any other similar identification credentials.	Appropriate GPSD Identification Office	*NRRS 1/105A Destroy credentials 3 months after return to issuing office.
14	Identification Credentials Files Receipts, Indices, Listings, and Accountable Records.	Appropriate GPSD Identification Office	*NRRS 1/105B Destroy after all listed credentials are accounted for.
15	Records of Acquisition of Firearms	Appropriate GPSD Security Contract Program Manager	*NPRS 1/106A Destroy 1 year after firearm is destroyed or transferred.
16	Certificate to carry firearms (NASA Form 699A and 699B)	Center Chief of Protective Services	*NPRS 1/106B Destroy 1 year after termination of certificate.
17	Firearms data relating to individual qualifications, training, and maintenance of proficiency in the use of firearms.	Appropriate GPSD office	*NRRS 1/106C Destroy 1 year after termination of individual.
20	Security Violation Files relating to alleged violation of a sufficiently serious nature that are referred to the Department of Justice or Department of Defense (DOD) for prospective determination, exclusive of files held by those Departments responsible for making such determinations.	Appropriate GPSD office	*NRRS 1/108A Destroy 5 years after close of case.

21	Security Violation Files – All other offices and files, exclusive of papers placed in official personnel folders.	Appropriate GPSD office	*NRRS 1/108B Destroy 2 years after completion of final action.
28	Logs, Registers, and Control Files – Visitors	Appropriate GPSD office	*NRRS 1/114A Destroy 5 years after final entry or date of document, as appropriate.
29	Logs, Registers, and Control Files – Security Officers	Appropriate GPSD office	*NRRS 1/114B Destroy 2 years after final entry.
32	Surveys and Inspections of Government-Owned Facilities	Appropriate GPSD office	*NRRS 1/116A Destroy when 3 years old, or upon discontinuance of the facility, whichever is sooner.
33	Surveys and Inspections of Privately-Owned Facilities	Appropriate GPSD office	*NRRS 1/116B Destroy when 4 years old or when security cognizance is terminated, whichever is sooner.
34	Fire, Explosion, and Accident Investigative Files – Precedent or Unusual Cases	Appropriate GPSD office	*NRRS 1/119A Permanent – Retire to FRC when 5 years old. Transfer to NARA when 30 years old.
35	Fire, Explosion, and Accident Investigative Files – Routine Cases	Appropriate GPSD office	*NRRS 1/119B Destroy when 2 years old.

**NRRS – NASA Records Retention Schedules (NPR 1441.1)*

P.9 MEASUREMENT/VERIFICATION

a. GSFC's Center Director and the Center Chief of Protective Services (CCPS), or their designees, determine, implement, ensure, and document compliance with GPR requirements and applicable Federal regulations utilizing Agency mandated independent accreditation and assessment teams as well as other verification approaches that are tailored to meet the needs of the Center.

b. The Office of Protective Services (OPS) conducts functional reviews of the Centers in compliance with NPR 1600.1A, Section 2.17, conducting spot-checks and inspections to review Center compliance and implementation of mandatory requirements.

PROCEDURES

CHAPTER 1.0 Introduction and Responsibilities

1.1 Introduction

Requirements in this directive are derived from and support the requirements established in NPR 1600.1A, NASA Security Program Procedural Requirements.

1.2 Responsibilities

1.2.1 Individuals and organizations at GSFC shall comply with the specific responsibilities for personnel security identified in NPR 1600.1A. These responsibilities are identified for the following:

a. Center Director
b. CCPS
c. Program Managers, Line Managers, and Supervisors
d. Employees and contractors.

1.2.2 The Center Chief Counsel or designee shall advise the CCPS and GPSD staff on all legal matters, to include search and seizure, use of force, jurisdiction, constitutional law, evidentiary standards, due process, release of information, and other protective services related enforcement matters.

1.3 Waivers and Exceptions

1.3.1 Requests for Waivers or Exceptions to this GPR shall be requested in accordance with NPR 1600.1A, Chapter 1.

1.4 Violations of Security Requirements

1.4.1 Anyone who willfully violates, attempts to violate, or conspires to violate any regulation or order involving NASA's personnel security program is subject to disciplinary action up to, and including, termination of employment and/or possible prosecution under 18 U.S.C. §799, that provides fines or imprisonment for not more than 1 year, or both.

1.5 Imminent Security Threat or Safety Risk

1.5.1 The CCPS, Center Directors, and NASA Headquarters Operations Director, or their designees, shall order the temporary removal and/or denial of access to all NASA facilities of any person who violates NASA security requirements and whose continued presence on NASA property constitutes an imminent security threat or safety risk to persons or property. Circumstances of removal and/or denial of access will be articulated in a report to become a matter of official record.

1.5.2 Upon temporary removal, the removal authority will comply with the notification and process requirements defined in NPR 1600.1A, Section 2.5.

CHAPTER 2.0 Security Operations

2.1 Security Controls at GSFC

2.1.1 GSFC employees and contractors shall comply with the requirements of NPR 1600.1A.

2.1.2 Physical security controls and other measures used for the protection of persons and property shall be the responsibility of and administered by the GPSD.

2.1.3 Uniformed Security Force officers shall staff all entrances and gates to GSFC. Access entrances and gates may have deployable physical security barriers which are controlled by the Security Officers (SO) at that entrance. GSFC facilities, buildings, and projects designated as critical areas or having critical information or personnel shall be controlled by an electronic physical access control system (EPACS) or a SO.

2.1.4 All personnel accessing GSFC shall have and display a valid NASA or GSFC identification badge (ID) while on the Center or any of its component facilities.

2.1.5 All personnel operating privately or contractor owned vehicles on GSFC property shall have a valid driver's license which is recognized and/or has reciprocity with the state in which GSFC's facility is located.

2.1.6 All vehicles accessing GSFC shall be properly registered and insured in a state of the United States or in a diplomatic entity which is recognized and/or has reciprocity with the state in which GSFC's facility is located.

2.1.7 Overnight storage of personally owned vehicles on GSFC property is authorized while on official government business. Extended storage of personally owned vehicles requires approval of the building Facility Operations Manager (FOM) and GPSD.

2.1.8 The Goddard Auto Club is authorized overnight storage of club members personally owned vehicles only on the Center designated club parking l with approval of the club manager

2.2 Inspection of Persons and Property

2.2.1 Consistent with NASA's requirement to ensure appropriate protection for personnel, property, and facilities, NASA reserves the right to conduct an inspection of any person and property in his/her possession as a condition of admission to, continued presence on, or upon exit from, any NASA facility. Implementation of requirements, policy, and procedures for all aspects of this program shall be in accordance with 14 C.F.R. Part 1204, subpart 10.

2.2.2 NPR 1620.3, Physical Security Requirements for NASA Facilities and Property, Appendix C addresses items prohibited from NASA facilities. Where NASA facilities are located on a military installation or an area of concurrent/proprietary jurisdiction, NASA personnel are subject to their policies and procedures.

2.2.3 All entrances to NASA real property or installations shall be conspicuously posted with the following notices:

a. "CONSENT TO INSPECTION: Your entry into, continued presence on, or exit from this installation is contingent upon your consent to inspection of person and property."

b. "UNAUTHORIZED INTRODUCTION OF WEAPONS OR DANGEROUS MATERIALS IS PROHIBITED: Unless specifically authorized by NASA, you may not carry, transport, introduce, store, or use firearms or other dangerous weapons, explosives or other incendiary devices, or other dangerous instrument or material likely to produce substantial injury or damage to persons or property."

2.2.4 Security Police Officers (SPO) and SOs shall be trained on how to perform inspections and, with appropriate training, may use inspection tools and detection devices (mirrors, x-ray, and other sensing devices) and/or canines, as necessary.

2.2.4.1 Training for security personnel conducting searches shall include:

a. Appropriate search techniques for the type of vehicle being searched.

b. Key locations where devices or other contraband may be secreted.

c. Procedures for confiscating illegal or dangerous items, detaining of individuals, and referring incidents to NASA's Office of the Inspector General (OIG) or appropriate external law enforcement.

2.2.4.2 Such inspections shall be conducted in accordance with the following guidelines:

a. Consent to Inspection Notices shall be prominently posted at entrances to NASA Centers and Facilities. Language for these notices is contained in 14 C.F.R. §1204.1003, Subpart 10.

b. Only NASA security personnel or members of the installation's uniformed security force will conduct inspections. Such inspections will be conducted in accordance with guidelines established by the Assistant Administrator (AA), OPS.

c. Prior to undertaking an inspection, security personnel not in uniform shall present their NASA credentials to the subject of the inspection.

d. If, during inspection, an individual is found to be in unauthorized possession of items believed to represent a threat to the safety or security of the Center (e.g., Classified National Security Information (CNSI), weapons, drugs, or explosives), or other prohibited items described in NPR 1620.3A, Physical Security Requirements for NASA Facilities and Property, Appendix C, the items shall be confiscated, and the individual will be denied admission to or be escorted from the Center or detained at the scene as directed by the CCPS/CCS or his/her designee. The NASA OIG or appropriate local law enforcement authorities will be notified immediately.

e. If, during an inspection conducted pursuant to this subpart, an individual is in possession of U.S. Government property without proper authorization, that person will be required to relinquish the property to the security representative pending a determination on the proper authorization for the possession of the property or its removal from the installation. The individual relinquishing the property will be provided with a receipt for the property.

2.2.5 At Goddard, deliveries, packages, containers, etc., shall be processed through Central Receiving prior to being granted access to the Center. No delivery vehicle will be permitted on Center until it has been processed through Central Receiving. **EXCEPTION**: Deliveries that arrive during hours when Greenbelt's Central Receiving is not in operation may be pre-approved by GPSD. Contact GPSD for approval procedures.

a. Deliveries, packages, containers, etc., that meet size requirement for processing through x-ray equipment shall be scanned prior to delivery on Center.

b. Deliveries, packages, containers, etc., that are too large to fit through x-ray equipment shall be visually scanned and may be checked by Security Force canine detection teams prior to delivery on Center.

2.2.5.1 At WFF, all deliveries shall report to the Badging Office (Building N-1), or the Island Gate (rocket motors, assets, large Navy components), for inspection during the hours of 8:00 a.m. to 4:30 p.m. They are then processed per a. and b. above.

2.2.5.2 At GISS and IV&V, all deliveries are processed through GPSD personnel located at the front or rear entrances of the facility.

2.2.5.4 All deliveries by outside vendors, companies, organizations, etc., who do not have a valid GSFC visitor's badge, shall be met at GSFC's point of entry and escorted by a GSFC employee or contractor. Vehicles going directly to the Shipping and Receiving Warehouse are not required to be escorted.

2.3 NASA's GSFC Badging Program

2.3.1 GPSD shall issue and provide access Personal Identity Verification (PIV) badges and Non-PIV badges consistent with NPR 1600.4, Identity and Credential Management. These badges shall be initiated, processed and issued through NASA's Identity Management and Account Exchange (IdMAX) system.

2.3.2 GPSD shall issue and provide non-PIV for specific use at GSFC. Non-PIV or "Center Specific" badges issued by GPSD are not acceptable identification for access to other non-GSFC Centers.

2.3.3 CCPS authorizes the issuance period for non-PIV badges, however no badge expiration date

shall exceed 2 calendar years without a required badge renewal and the completion of appropriate investigation.

2.3.4 U.S. Citizen Visitor badges shall be requested 48 hours (2 business days) in advance, and shall be submitted to GPSD through established electronic processes (i.e., Electronic Management Operations Directorate (eMOD) or WIIMS) whenever possible. Users will comply with the designated approval requirements within the approved systems.

2.3.5 Unannounced/unexpected (i.e., less than 48 hours (2 business days) notice) U.S. Citizen visitors shall be escorted by a picture badged NASA or GSFC employee or contractor.

2.4 Foreign National (FN) Badging

2.4.1 Requests for FNs from non-designated countries shall be completely initiated in IdMAX at least 10 business days in advance and from designated countries at least 20 business days in advance. The Center International Visit Coordinator (IVC) can provide a list of designated countries.

2.4.2 Sponsors shall submit all appropriate forms and documentation within IdMAX for consideration for access by the submission deadlines. The request information will be reviewed by Chief Information Officer (CIO) for IT Security (for IT system access), the IVC, the Center Export Control (HQ OIIR for Designated Countries) official, and CCPS prior to a decision being made for physical and logical access.

2.4.3 GSFC non-PIV FN badges shall be one of the following:

a. **ESCORT REQUIRED** – valid for access only with an authorized NASA or GSFC civil servant or contractor US citizen pictured badged employee acting as escort, whose attendance to the visitor is mandatory at all times while on Center;

b. **LIMITED ACCESS** – valid only for access during normal weekday duty hours (6:00 a.m. to 6:00 p.m., Monday-Friday). No weekend or holiday access is authorized, except with prior approval and an escort;

c. **UNESCORTED/UNLIMITED ACCESS FN VISITOR** – valid for access to GSFC and its facilities during normal duty hours, after hours, weekends, and holidays. It indicates that the individual has successfully met the security requirements;

d. **UNESCORTED/UNLIMITED ACCESS FN EMPLOYEE OR CONTRACTOR** – valid for GSFC FN employees or contractors, providing access to GSFC and its facilities during normal duty hours, after hours, weekends, and holidays. It indicates that the individual has successfully met the security requirements. The individual must be a valid GSFC employee, contractor, tenant employee, grantee, etc.

2.5 Badge Display and Access

2.5.1 All badges shall be worn and visibly displayed at all times while the badge holder is on GSFC property. Badges will be worn photo and name-side visible and above the waist.

2.5.2 No symbol, pin, decal, sticker, or other device shall be affixed to any ID badged. GPSD issued Emergency Personnel stickers may be affixed to the badge holder but shall not obstruct the clear view of the badge.

2.5.3 All NASA and GSFC badges are the property of the U.S. Government and shall be surrendered upon request of GPSD.

2.5.4 The badge holder shall:

a. Ensure that the badge is safeguarded at all times;
b. Ensure that the badge is not defaced or damaged;
c. Immediately report the loss, theft, duplication, or forgery of any NASA PIV or non-PIV ID badge to GPSD;
d. Challenge anyone seen on GSFC without a proper, valid badge, or immediately report that fact to GPSD;
e. Notify GPSD of any name change;
f. Surrender the ID badge upon resignation, termination from employment or denial of access by CCPS.

2.5.5 GPSD shall issue NASA retiree ID badges to civil service employees retiring from GSFC.

2.6 Exceptions to NASA PIV and/or Non-PIV Issuance

2.6.1 The following situations may not warrant issuance of a NASA PIV or a non-PIV Badge:

a. Children under the age of 16, as long as they are sponsored and accompanied by a parent, legal guardian, or other authorized holder of a NASA PIV or GSFC Non-PIV badge with a photo. Actions of all children granted access under this provision shall be the responsibility of the adult sponsoring the visit.

b. Vendors (e.g., deliverers of fuel, laundry, vending machine foods, bulk liquid gases like liquid nitrogen, etc.) who do not meet the contract requirements for badge issuance may be permitted access to GSFC if a specific written request is submitted to GPSD by the requesting organization. The request shall include appropriate justification for "frequent" access, the vendor's name, verification of U.S. citizenship of the "typical" driver(s), frequency of access, and impact if the particular vendor is not permitted "routine" access to the Center. The request will be reviewed and approved, or disapproved with explanation, by CCPS or designee.

c. Vendors who routinely service GSFC on a regular basis, i.e., more than 3 days a week (e.g., oil deliveries, liquid nitrogen deliveries, United Parcel Service, Federal Express, vending services, etc.), may be issued a non-PIV badge if they meet the Center's eligibility requirements. Any vendor that does not qualify for a GSFC-specific badge will be badged as a visitor.

d. Construction contractors and their subcontractors are authorized access by virtue of their contract and the specific authorization of the contracting officer and contracting officer's representative. Only those contractors/subcontractors who will be physically located on GSFC for the duration of the contract may be issued NASA PIV. All other contractors/subcontractors shall be issued appropriate NASA GSFC non-PIV badges access badges valid for the duration of the particular function or construction project they are working on. Construction contractors may receive temporary badges valid for up to 6 months, if they meet the Center's eligibility requirements, and these badges may be renewed with proper authorization.

e. All service of papers/process shall be coordinated through GPSD with guidance from the Office of Chief Counsel. GPSD is not authorized, or permitted, to accept process service for individuals, companies, or the U.S. Government.

f. Special Agents and Investigators with valid credentials from other Federal agencies conducting non-emergency official business or inquiries on GSFC may be allowed access to the Center based on their credentials. At the discretion of GPSD, they may be issued a valid non-PIV or visitor ID badge.

g. Attendees of special activities, conferences, or other special functions shall obtain and display a "Special Events" badge approved by GPSD, which has the date(s) of activity duration, name or acronym of the activity, and a place for the attendee's or holder's name. The attendee or badge holder shall complete the "name" section and display the badge conspicuously throughout the duration of the event or activity.

2.8 NASA Security Areas

2.8.1 NASA shall establish security areas as defined in 14 C.F.R. Part 1203a. These types of security areas include Controlled Area, Limited Area, Exclusion Areas.

2.8.2 Establishment, Maintenance, and Revocation of security areas at GSFC shall comply with NPR 1600.1A, Section 2.7.

2.9 Standards for Secure Conference Rooms

2.9.1 When established as permanent facilities, NASA Secure Conference Rooms shall meet security standards outlined in Director National Intelligence (DNI) Intelligence Community Directive (ICD) Number 705.

2.9.2 At a minimum, NASA Secure Conference Rooms shall be identified as NASA Limited Areas.

2.9.3 Classified meetings held in rooms not configured in accordance with ICD 705 shall comply with NPR 1600.1A, Section 2.8 and NPR 1600.2.

2.10 Technical Surveillance Countermeasures

2.10.1 Technical Surveillance Countermeasures support shall be provided by GPSD CI Section and coordinated through NASA Headquarters' Director, Security Management Division.

2.11 Facility Security

2.11.1 GPSD shall conduct a Physical Security Vulnerability Risk Assessment on each building at GSFC as required and specified in NPR 1620.2A.

2.11.2 A representative from GPSD shall be part of, and involved in, all new construction projects, major renovations of facilities or buildings, and/or organizational renovations, moves, or reorganizations. New construction and renovations shall comply with security requirements as defined by GPSD for locks and locking devices, master key systems, EPACS devices, and other security requirements as defined or developed for the construction or renovation project.

2.11.3 GSFC facility construction projects, renovations, repairs, or other facilities projects shall meet the physical security standards and requirements as defined by NPR 1620.3A for fences, locking devices, key systems, EPACS devices, security alarms, building-to-parking lot or roadway setbacks, etc., for protection of personnel, property, equipment, resources, etc.

2.11.4 GSFC key control procedures implement the requirements of NPR 1620.3A, and are described in Chapter 7 of this GPR.

2.12 Unauthorized or Restrictive Activities

2.12.1 The following are unauthorized or restricted activities at GSFC or any of its locations:

2.12.2 Possession of Contraband and Drugs and Consumption of Alcoholic Beverages

2.12.2.1 The possession of contraband, i.e., goods or materials that are illegal to possess, is prohibited on GSFC. Illegal drugs (as defined by the Drug Enforcement Administration) are prohibited on any GSFC location. Persons prescribed narcotic-type medical drugs shall carry them in approved containers with a valid prescription label affixed to the container.

2.12.2.2 Alcoholic beverages may be served by and consumed at the Greenbelt Recreation Center and WFF Rocket Club, and at other Greenbelt and WFF locations upon approval of the appropriate Division Chief during non-duty hours with notification to GPSD for safety and security purposes. Transportation

of open containers of alcoholic beverages shall comply with the laws of the surrounding local jurisdiction.

2.12.3 Intoxicated Individuals

2.12.3.1 Entering the GSFC, or operating a motor vehicle on GSFC property at any GSFC facility, while under the influence of intoxicating beverages or legal/illegal drugs that impair driving ability is prohibited. Individuals determined to be intoxicated or with impaired driving ability will be denied entrance or removed/escorted from GSFC, as the situation warrants. If already on GSFC, their keys and badges may be confiscated, law enforcement officials may be called, and they may be removed or escorted from GSFC, as the situation warrants. Keys will be returned when the individual meets the legal requirements to drive.

2.12.4 Hunting and Fishing

2.12.4.1 There is NO hunting allowed at GSFC. At Greenbelt, fishing is restricted to members of the Government Employees Welfare Association (GEWA) Fishing Club and only under approved club rules. At WFF, fishing is prohibited on Wallops Island during WFF launch operations and on the Main Base at all times. Fishing is permitted on Wallops Island at other times by individuals with a NASA photo-ID or GSFC non-PIV badge. No fishing permit is required to fish on Wallops Island; State of Virginia laws apply.

2.12.5 Ice Skating

2.12.5.1 There is no ice skating allowed at, or on, GSFC properties.

2.12.6 Photographic and Recording Equipment

2.12.6.1 The possession and use of photographic, video, and/or sound recording equipment on GSFC is prohibited within Limited areas, Exclusion areas, and NCI facilities (as defined in NPR 1600.1A) without prior approval of GSFC CCPS.

2.12.6.2 Use of photographic, video, and/or sound recording equipment shall comply with NPD 2530.1G, Monitoring or Recording of Telephone or Other Conversations. Operation of photographic, video, and/or recording equipment shall be in an open, public manner so that all personnel involved are aware of its use and function. Approval of the Chief Counsel or his designee shall be obtained prior to use of any video or audio recording device whose use is not open and known and clearly disclosed to personnel being recorded (e.g., surveillance activities). Custodians of classified material and technical monitors of classified tests and operations are responsible for ensuring that classified materials and/or information are protected from unauthorized disclosure through recording or photographic activities.

2.12.6.3 Official news media personnel may carry photographic, video, and/or sound recording equipment on the GSFC, except in areas where prohibited, provided they are escorted by an authorized

representative of the Office of Communication (OOC). It is the responsibility of the OOC to escort and/or the person visited, interviewed, or photographed to ensure that no unauthorized photographs or recordings are made and that there is no compromise of classified information.

2.12.7 Gambling

2.12.7.1 Employees shall not conduct, or participate in, any gambling activity including the operation of a gambling device, conducting a lottery or pool, a game for money or property, or selling or purchasing a numbers slip or ticket.

2.12.8 Solicitation

2.12.8.1 Except as authorized by the Center Director, GEWA or Wallops Exchange and Morale Association, individuals shall not engage in commercial solicitation at GSFC, such as distribution of commercial advertising material or product samples, or collecting debts. Fundraising, except for the Combined Federal Campaign, is prohibited. Approved activities and the collection of commercial debts by authorized financial institutions (e.g., NASA Federal Credit Union) are permitted. Sales and marketing representatives on official business with NASA will be permitted to call on clients at GSFC on a by appointment only basis.

2.12.9 Animals

2.12.9.1 No domesticated animals, except trained assistance dogs and dogs brought in for official purposes, are permitted on GSFC or its facilities. Employees, contractors, and guests on GSFC will not feed or attempt to domesticate any of the wild animals inhabiting GSFC properties or facilities. Employees, contractors, or guests who discover dangerous, annoying, dead or dying animals on GSFC should immediately report the event or situation to GPSD.

2.12.10 Children

2.12.10.1 Children of GSFC civil service employees, GSFC contractor employees, personnel completing work through Space Act Agreements, Memorandum of Agreement (MOA), or Memorandum of Understanding (MOU), those assigned or detailed under the Intergovernmental Personnel Act, partners, recipients of grants and cooperative agreements, and visitors may be permitted on GSFC facilities if they are escorted by their parent(s) or guardian(s). Children may be left at the Child Development Center for child care purposes with the approval of the Child Development Center.

2.12.10.2 Except as provided above, children shall be accompanied and controlled by their parent(s) at all times. Children creating a disruption in the workplace shall be reported to a supervisor or GPSD. Children are considered to be visitors and may not be taken into Limited areas or Exclusion areas (see NPR 1600.1A) without prior written approval and authorization by the area owner. Similarly, ethics regulations and other policies may restrict the access of children at non-official activities, such as child care while on government duty, or that local managers may impose.

2.13 Flight and Launch Site Security

2.13.1 All GSFC aircraft and other flight operations (balloons, unmanned aerial vehicles, rockets, etc.) shall comply with the requirements of NPR 1600.1A, NPR 1620.2A and NPR 1620.3A.

2.13.2 GPSD will establish, coordinate and maintain operational security for flight and launch operations at GSFC. This shall include development and implementation of an operational plan for visitor control, law enforcement response, and emergency management response. GPSD shall coordinate outside agency or local government response resources.

2.13.3 All GSFC directorates involved in suborbital flight and rocket launch operations shall coordinate with the appropriate security office to ensure that documented procedures are in place to meet the requirements of NPR 1600.1A, NPR 1620.2A and NPR 1620.3A for all flight missions.

2.13.4 All GSFC sites shall have appropriate plans and procedures for landing and takeoff of emergency assistance aircraft, e.g., helicopters, at or near the facility, for emergency medical evacuations or other emergency situations. At GSFC the requirements are specified in GPR 6500.1.

2.13.5 WFF has an established airfield onsite. WFF Security Office shall be responsible for all airfield and aircraft security matters on the WFF airfield.

2.14 Security Threat and Incident Reporting

2.14.1 With the exception of one small tract of undeveloped land to the west of the Baltimore-Washington Parkway, the Greenbelt facility has exclusive Federal jurisdiction; therefore, State and local law enforcement agencies have no law enforcement jurisdiction on the vast majority of the facility. GSFC shall seek to maintain a MOU with the U.S. Park Police (USPP) to provide law enforcement support at/on the Greenbelt facility when requested. When called, USPP has law enforcement authority as stated in the MOU and will work with GPSD representatives and GSFC Security Force to the successful conclusion of the incident or situation.

2.14.1.1 WFF's facility, depending on the specific location, has either exclusive Federal jurisdiction or concurrent jurisdiction with local and state law enforcement agencies. GSFC shall seek to establish and maintain an MOU similar to that described in paragraph 2.14.1 of this GPR with local and state law enforcement agencies to define authority and responsibility for responding to incidents, situations, demonstrations, etc..

2.14.1.2 IV&V's facility is part of the University of West Virginia (UWV) and is located on state land. GSFC shall seek to establish and maintain contractual arrangements with UWV to define authority and responsibility for responding to incidents, situations, demonstrations, etc.

2.14.1.3 GISS facility is located in a Government Services Administration (GSA) facility. GSFC shall seek to establish and maintain an MOU similar to that described in paragraph 2.14.1 of this GPR with GSA to define authority and responsibility for responding to incidents, situations, demonstrations, etc.

2.14.2 All incidents of threats, thefts, crimes or suspected criminal activities, emergencies, serious injuries, fires, etc. on GSFC or NASA facilities, except IT security incidents, shall be reported to GPSD. This is in addition to the mishap reporting requirements of GPR 8621.1. Refer to GPR 2810.1 for IT security incident-handling procedures.

2.14.2.1 Examples of reportable incidents are:

- possible espionage,
- possible sabotage,
- suspicious packages,
- suspected terrorist activities,
- bombing incidents (including bomb threats),
- shootings or other violent acts,
- destruction of NASA facilities, property, or equipment,
- death or serious bodily harm requiring hospitalization,
- threats against NASA property, missions, or personnel,
- information regarding concealment of firearms, explosives, or implements of war, and
- information regarding individuals appearing to act irrationally in efforts to contact NASA or other high officials in the U.S. Government.

2.14.2.2 Employees and contractors shall be responsible for immediately reporting all security incidents (see Paragraph 2.14.2.1 of this GPR) to GPSD.

2.14.2.3 Employees and contractors shall be aware of **Espionage and Terrorism Indicators** information listed on Appendix C of this GPR, and shall immediately report suspicious activity to the OPS CI Special Agent assigned to GSFC.

2.14.2.4 Any GSFC employee or contractor who observes any incident involving fraud, waste and/or abuse shall report it to the OIG, as required by NPD 9800.1B.

2.14.2.5 GSFC CCPS will maintain statistics for areas identified in NPR 1600.1A, Appendix C, Property Loss and Incident Details. This information will be sent to the AA, OPS quarterly and/or as requested.

2.15 Investigations

2.15.1 The investigative component of GSFC PSD is directly related to the security and protection mission and may include inquiries into such matters as threats or occurrences of workplace violence, harassment, eligibility and suitability for Homeland Security Presidential Directive (HSPD)-12 requirements, missing or stolen property, misuse of government property, unauthorized access, and other violations of NASA and Center security policies.

2.15.2 Employees and contractors shall cooperate with all GPSD investigations into security incidents, and provide any requested assistance and relevant information to authorized investigators. All supervisors shall advise their employees and contractors of their duty to cooperate with GPSD investigative efforts.

2.15.3 GPSD shall review each reported security incident or security violation and determine the need for further investigation. Decisions to investigate security incidents or violations will be made after consideration of applicable Federal and state laws and consistent with designated GPSD and OIG investigative responsibilities.

2.15.4 GSFC CCPS shall closely coordinate investigative activity with the appropriate internal and external organizations (e.g., OIG, CIO, Office of Human Capital, Office of the Chief Counsel, EEO, Federal Bureau of Investigation , Bureau of Alcohol, Tobacco, Firearms and Explosives, DoD, and local and state police) to ensure that cases are referred to the appropriate organization for follow-up when this is required.

2.15.5 GSFC CCPS shall coordinate the release of information concerning reported missing and stolen controlled Government property with the Center Logistics Management Division on a quarterly basis to ensure accountability of controlled property and compliance with NPR 4200.1, NASA Equipment Management Procedural Requirements.

2.15.6 Information received and documented in a GPSD investigative report often involves personal data and law enforcement information that is sensitive in nature, the release of which may be limited or prohibited by Federal laws, such as the Privacy Act and Freedom of Information Act (FOIA). Privacy Act requests for documents by personnel with an official need to know the information, as well as requests by employees seeking information about themselves, shall be submitted to the CCPS. Other requests for GPSD documents under the FOIA shall be submitted to the Center FOIA Office.

2.16 Dealing with Demonstrations

2.16.1 All planned or impromptu demonstrations or strikes/informational labor picketing at any GSFC location, that affect NASA interests, shall be reported to GPSD as soon as they become known.

2.16.2 The GPSD will respond to all such incidents, and set up an incident command post, establish perimeter access control at the point of the incident, and notify GSFC's OOC and other appropriate GSFC management.

2.16.3 GSFC CCPS shall make reasonable efforts to safely manage groups or crowds who have assembled. CCPS should make appropriate liaison and coordination with local law enforcement, and/or adjacent Federal agency facilities.

2.17 NASA National Terrorism Advisory System (NTAS) Program

2.17.1 NASA NTAS program is designed to meet the requirements of the NTAS developed and implemented by the Department of Homeland Security (DHS).

2.17.2 GSFC will utilize NASA NTAS; associated actions are outlined in NPR 1600.1A, Appendix D, NASA NTAS Actions.

2.17.3 The alert system types range from "No Current Alerts" (normal operating security policy), "Elevated Threat Alert," and "Imminent Threat Alert."

2.17.4 The alert system is intended to standardize terms and establish standardized security measures that can be initiated by the AA, OPS and Center Directors through the Agency-wide emergency notification system.

2.17.5 GSFC components hosting military organizations as tenants, residing as a tenant on a military installation, or situated contiguous to a military installation shall establish mutually agreed upon notification systems for ensuring DoD's use of ALPHA designators under the DoD Force Protection Condition concept are understood and integrated into the Center's threat condition warning system.

2.18 Hazardous Material (HAZMAT) Security

2.18.1 NASA programs use many different hazardous materials in meeting mission objectives. It is imperative that the use, storage, and protection of these materials be given the highest priority necessary to ensure the safety of NASA personnel and the general public.

2.18.2 All HAZMAT brought to, or transported on, the Greenbelt facility shall be processed through Central Receiving and the security checkpoint for deliveries in the Building 35 Warehouse. HAZMAT deliveries made to the Greenbelt facility after Central Receiving is closed may, with prior approval, be processed by GPSD personnel upon arrival. Contact GPSD for approval procedures.

2.18.3 HAZMAT deliveries to WFF shall report to WFF's Main Gate for inspection Monday through Friday only, excluding holidays, during the hours of 8:00 a.m. to 4:00 p.m.; others will be turned away unless other arrangements are made in advance. IV&V and GISS do not receive HAZMAT deliveries.

2.18.4 All HAZMAT carrier vehicles shall be inspected by GPSD's SO.

2.18.5 All HAZMAT deliveries made directly to the Greenbelt facility or WFF shall be escorted by a NASA or GSFC employee or contractor of the organization receiving the shipment, or shall have prearranged for a Security escort.

2.18.6 HAZMAT shall be stored, maintained, and used in such a manner as to prohibit access and/or use by unauthorized personnel. Storage containers and facilities housing HAZMAT shall be protected with appropriate access control devices (e.g., EPACS or restricted locks and keys), blast- or explosive-

resistant barriers, fences, etc., to ensure that only authorized personnel have access and that accidental explosion, disbursement, and/or contamination is contained.

2.19 Security Education, Training, and Awareness (SETA) Program

2.19.1 Responsibilities

2.19.1.1 GSFC's Center Director shall ensure that adequate procedures are in place whereby all NASA employees and contractor personnel, regardless of clearance status, are briefed annually regarding Center security program responsibilities.

2.19.1.2 GSFC's CCPS shall ensure that appropriate and knowledgeable security personnel provide and receive the applicable types of briefings or training, as described in paragraph 2.19.2 of this NPR.

2.19.1.3 NASA supervisors shall ensure job-related, facility-oriented security education and awareness instruction or training for newly assigned personnel are timely and properly coordinated with GSFC's CCPS.

2.19.2 Required Briefings and Training.

2.19.2.1 Initial Orientation Security Briefing. This briefing shall be given by GPSD personnel (i.e., NASA and/or security services contractor) to acquaint new employees with local security procedures and employee responsibilities to protect personnel and to protect Government property from theft, loss, or damage. Orientation briefings should include, but are not limited to, general discussions on:

a. Access/entry and exit control procedures and responsibilities
b. Property accountability responsibilities
c. Pilferage control
d. Identification of restricted areas
e. Use and security of identification credentials
f. Key and lock control procedures
g. Protection of CNSI and/or SBU (includes Personally Identifiable Information (PII), For Official Use Only information, other privacy act information, and sensitive operational information).
h. Emergency reporting procedures
i. Reporting security violations and/or suspicious activity
j. Orientation to the local area and criminal trends

2.19.2.2 Annual Security Training. This training is designed to sustain an appropriate level of awareness throughout the workforce and reinforce the security policies and procedures outlined in initial orientation training.

2.19.2.3 Supervisory Security Briefing. Security orientation briefings shall be given by the responsible supervisor or designee to each new employee and will include all security requirements and procedures for which the employee is to be specifically responsible.

2.19.2.4 Security Clearance Briefing. GSFC's CCPS will ensure the appropriate security indoctrination briefing is given to each employee prior to that employee receiving a personnel security clearance and being granted access to classified information.

2.19.2.4.1 Annual Security Clearance Refresher Briefing. GSFC's CCPS will ensure the appropriate security clearance refresher briefing is given to all NASA personnel and contractors possessing a security clearance and performing work on NASA classified programs. Initial and annual refresher briefings are also required for individuals granted accesses to certified National Security Systems that process classified information. Clearances may be suspended or revoked for failure to complete annual training.

2.19.2.4.2 CNSI Custodian Briefing. GSFC's CCPS will ensure classified material custodians and any other custodians responsible for CNSI security containers, records, or facilities are given initial and annual refresher briefings by security personnel regarding their specific responsibilities for safeguarding classified information.

2.19.2.4.3 CNSI Termination Briefing. GSFC's CCPS will ensure security termination briefings are given to employees whose personnel security clearances are being terminated due to termination of employment, transfer to another Center, or if the individual no longer requires access to CNSI. This briefing is designed to ensure termination of all classified activity and holdings by the employees and remind them of their life-long responsibilities and penalties for unauthorized disclosure of CNSI even after termination of the clearance or employment.

2.19.2.4.4 GSFC's CCPS will ensure other special security training or briefings are given to employees related to Special Access Programs, Sensitive Compartmented Information , and NASA Critical Infrastructure (NCI).

2.19.2.5 Foreign Travel Briefings. NASA Headquarters OPS CI personnel shall conduct foreign travel briefings at GSFC to NASA travelers to enhance their awareness of potential hostile intelligence, terrorist, and criminal threats in the countries to which they are traveling. These briefings must also provide defensive measures and other practical advice concerning safety measures.

a. NASA GSFC employees shall report to the Center or Agency CI Office any meetings with foreign nationals from designated countries that are held outside NASA-controlled facilities in advance of the meeting.
    1) NASA employees attending the meeting will make themselves available for intelligence threat awareness pre-briefings and debriefings in accordance with NPD 1660.1B. The Center IVC can provide a list of designated countries.

2.19.2.6 GPSD shall provide both security awareness and guidance to projects and programs regarding protection of unclassified sensitive mission information or technologies. The information provided to programs and projects will be based on industry best practices and real-life lessons learned with the Agency.

2.20 NASA OPS Functional Reviews

2.20.1 GSFC's PSD shall participate in the ongoing NASA OPS Functional Review Program to ensure that each Center is implementing their Protective Services programs in accordance with all applicable NASA and Federal regulations and to identify areas that need to be addressed that are not in compliance with appropriate rules and regulations.

2.20.2 This program shall include the periodic review and assessment at each NASA Center of the Information, Industrial, Personnel, Physical Security, Program Security, Emergency Management, Protective Services Contract Review, and Continuity of Operations.

CHAPTER 3.0 NASA Critical Infrastructure (NCI) and Program Security

3.1 NCI and Key Resources Identification, Prioritization, and Protection

3.1.1 PPD-21 "Critical Infrastructure Security and Resilience" directs every Government agency to establish a program to identify critical essential infrastructure and key resources, evaluate these assets for vulnerabilities, and fund and implement appropriate security enhancements (procedural and physical) to mitigate vulnerabilities. NASA has elected to designate its critical infrastructure and key resources as NCI to better facilitate designation of vital "mission oriented" critical infrastructure and key resources.

3.1.2 Criteria and procedures NASA Centers shall use in identifying NCI are contained in NPR 1600.1A, Appendix F, Identifying and Nominating NASA Assets for the NASA Critical Infrastructure Protection Program (NCIPP).

3.1.3 Minimum security requirements for NCI facilities or facilities housing NCI assets are provided in NPR 1620.3A, Physical Security Requirements for NASA Facilities and Property.

3.2 Risk Management Process

3.2.1 NASA has adopted a risk management approach, using requirements established in NPR 8000.4A, Agency Risk Management Procedural Requirements, NPR 1620.2A, Facility Security Assessments, and NPR 1620.3A, Physical Security Requirements for NASA Facilities and Property, in which the risk must be weighed against the cost and operational impact of implementing established minimum-security standards.

3.2.2 The CCPS shall ensure that security and program standards established in this GPR and other NPRs are met, or that appropriate requests for exception or waivers are submitted.

3.3 Program Security

3.3.1 Major GSFC functional organizations or directorates shall each designate a Security Program Manager to coordinate the implementation of the requirements of this GPR within their organizations. Similarly, GPSD may require organizations owning or responsible for certain special facilities to designate a Facility Security Manager with similar responsibilities. Names and contact information for Security Program Managers and Facility Security Managers shall be provided to GPSD by the responsible organizations and shall be maintained up to date.

3.3.2 GSFC programs shall utilize a system security approach in the development of a NASA program or in enhancing the protection level of an active program.

3.3.3 Programs shall identify security provisions as early as possible in system designs, acquisitions, or modifications, thereby minimizing costs, vulnerabilities, and compromises.

3.3.4 GSFC's CCPS is responsible for the following:

a. Establishing systems that ensure security requirements and provisions are identified at the outset of new or changing programs, acquisitions, and modifications.
b. Incorporating appropriate security measures, outlined in the various chapters of this GPR and others, into project plans, facility plans, construction and modernization projects, and requests for proposals impacting program security.

3.3.5 Project and program managers are responsible for the following:

a. Ensuring provisions contained in NPR 7120.5E, NASA Space Flight Program and Project Management Requirements, are appropriately addressed with CCPS.

b. Ensuring that critical programs or assets are identified for inclusion on the consolidated inventory and that program planning includes security provisions and funding.

c. Reporting incidents or perceived incidents involving loss of sensitive mission information to GPSD.

3.4 OPSEC

3.4.1 NSDD 298: National Operations Security Program establishes the National OPSEC Program and requires executive departments or agencies supporting national security classified or sensitive missions to establish a formal OPSEC program.

3.4.2 OPSEC measures shall be applied on all NASA classified programs.

3.4.3 If OPSEC planning is warranted, program and project managers, in coordination with GSFC PSD, shall develop and implement a project OPSEC plan that will identify critical information or activity, analyze threat(s) and vulnerability(ies), assess risk, and apply appropriate countermeasures.

3.4.4 No information system can process classified information until a System Security Authorization Agreement is in place. A requestor acquires this approval through their management and the Center Director. The Center Director's approval then allows PSD to proceed and provide the necessary Certification and Accreditation of the information system.

3.4.4.1 The classified information processing approval process is as follows:

a. The program, project, or other requesting organization shall submit a request memo to CCPS describing what kind of classified information they need to process, why they need to process it, and the computer system or network proposed for the activity.
   1) The requesting organization shall not purchase/acquire computer equipment prior to receiving CCPS's recommendations.
   2) The request memo requires Division level approval.

b. If CCPS approves the request, it will be routed to the Center Director for approval.
c. If approved by the Center Director, CCPS will coordinate the Certification and Accreditation Process, resulting in a System Security Authorization Agreement.

3.5 Special Security Programs

3.5.1 All NASA security activity associated with Special Security Programs are authorized and prescribed by NASA's Special Access Program Security Guide (SAPSG). Furthermore, NPD 1600.4, National Security Programs, establishes policy for Special Access Programs (SAP).

CHAPTER 4.0 Control, Issuance, and Storage of Arms, Ammunition, and Explosives (AA&E)

4.1 Authority

4.1.2 Under authority delegated from AA, OPS, GSFC CCPS shall direct or grant approval for their Center's NASA Special Agents and designated NASA Security Specialists and contractor security personnel to carry firearms. CCPS will withdraw weapons-carry authority for any NASA Special Agent, Security Specialist, or Armed SPO/SO if deemed in the best interest of the Agency, and shall notify the AA, OPS as soon as practicable of the action taken and the basis for taking the action.

4.2 Responsibilities

4.2.1 GSFC CCPS, NASA employees and contractors shall comply with the responsibilities identified in the requirements described in NPR 1600.1A, Chapter 4.

4.3 Authorization to Carry Firearms

4.3.1 GSFC CCPS shall only authorize the carrying of firearms in compliance with NPR 1600.1A, Chapter 4.

4.4 Carrying Weapons On Commercial Aircraft

4.4.1 Armed NASA Special Agents shall carry firearms on aircraft in compliance with NPR 1600.1A, Chapter 4.

4.5 Firearms Instruction

4.5.1 The certifying official (AA, OPS or GSFC CCPS when so delegated) shall designate a firearms instructor in compliance with NPR 1600.1A, Chapter 4.

4.6 Training

4.6.1 GSFC PSD NASA Special Agents shall be trained and certified in compliance with NPR 1600.1A, Chapter 4.

4.7 Maintenance of Proficiency

4.7.1 NASA Special Agents, Security Specialists, and security contractors authorized to carry firearms shall qualify with their issued firearm and receive annual testing and training on the simulator, non-lethal training ammunition (e.g., "Simunition") or other approved methods of judgmental shooting in compliance with NPR 1600.1A, Chapter 4.

4.8 Records

4.8.1 GSFC law enforcement training originator shall maintain records of personnel certified to carry firearms, including the basis for qualification, qualifying scores, rounds fired, and all other pertinent data in compliance with NPR 1600.1A, Chapter 4.

4.9 Firearms Standards

4.9.1 The CCPS shall utilize only firearms listed in the NASA Approved Firearms List (AFL) to arm civil service and contractor security staff in compliance with NPR 1600.1A, Chapter 4.

4.10 Weapons

4.10.1 NASA GSFC Protective Services contractor personnel and civil service personnel shall only carry weapons in compliance with NPR 1600.1A, Chapter 4.

4.10.2 Firearms (e.g., handguns, rifles, machine guns, shotguns, and ammunition) or other intermediate levels of force devices (e.g., Oleoresin Capsicum (OC) spray (pepper spray), tear gas and batons) are only authorized on GSFC property as follows:

a. NASA employees or contractors who hold NASA Headquarters certifications to possess the required firearms or intermediate level of force device;
b. Employees of other Federal agencies who are authorized and required by their agency to carry firearms or other intermediate levels of force devices in the performance of their duties; or
c. State and local law enforcement officers required to be armed or carry intermediate levels of force devices in the performance of their duties.

4.11 Exchange of Weapons

4.11.1 GSFC PSD weapons shall be stored, issued, returned, exchanged and inspected in compliance with NPR 1600.1A, Chapter 4.

4.12 Firearm Maintenance

4.12.1 All GSFC PSD firearms shall be periodically inspected and kept in good working order by a qualified gunsmith/armorer.

4.13 Ammunition

4.13.1 GSFC PSD shall issue and expend ammunition in compliance with NPR 1600.1A, Chapter 4.

4.14 Accountability of Arms, Ammunition, and Explosives (AA&E)

4.14.1 The accountability of AA&E at GSFC shall be in compliance with NPR 1600.1A, Chapter 4.

4.14.2 At all GSFC facilities, the PSD may use detection devices and/or canine detection teams to perform routine inspections, RVIs, delivery inspections, and package inspections. In addition, the PSD shall respond to all incidents, threats, or reports of firearms, ammunition, or explosives violations on those facilities.

4.15 Storage of AA&E

4.15.1 Firearms and ammunition shall be stored in accordance with NPR 1620.3A, Physical Security Requirements for NASA Facilities and Property, Section 3.17.

4.15.2 Certain GSFC organizations may be required to store, maintain, and handle explosives in the performance of their duties. Organizations at GSFC who deal with arms, ammunition and/or explosives, electro-explosive devices, pyrotechnic devices, and propellants, including rocket fuel and motors, shall provide GPSD a list of the types of these explosives, locations where stored, and a list of all personnel

who use or transport them in the performance of their duties. The list will include individuals' names, organization codes, phone numbers, types of explosives to be used, location, name of mission(s) supported, and storage locations of explosives. Applicable GSFC organizations shall update this list quarterly and submit to their respective PSD offices.

CHAPTER 5.0 NASA Protective Services Office Special Agent and Security Specialist Badges and Credentials (B&C)

5.1 Badge & Credential Use

5.1.1 NASA Credentials will be issued and returned in accordance with NPR 1600.1A, Chapter 5.

5.1.2 Only to those civil service protective services employees who are required to present proof of their authority in the performance of their official duties shall be issued badges and credentials.

CHAPTER 6.0 NASA Armed Personnel Training, Certification, and Authority

6.1 51 U.S.C. § 20133 authorizes NASA's Administrator to prescribe security regulations in support of these regulations and as approved by the Attorney General of the United States. NASA's Administrator also prescribes statutory FAA. Those regulations are set forth in 14 C.F.R. Part 1203b.

6.2 All NASA Special Agents, Security Specialists, and contractors assigned as NASA SPOs and NASA SOs shall comply with the training, certification and authority requirements of NPR 1600.1A Chapter 6.

6.3. GSFC CCPS shall ensure that prior to the issuance or the mandated use of any security equipment that an evaluation by NASA Protective Services Training Academy (NPSTA) for compliance and application within the use of force training requirements.

6.3.1 Specialized equipment requiring evaluation includes any firearms, Electronic Control Devices (ECD), K9 Explosive Ordnance Detection (EOD) services, vehicle inspection equipment, narcotics identification and detection equipment, OC spray, batons, and other special control equipment or duty gear that require use of force application and training considerations.

CHAPTER 7.0 Locks, Keys, and Electronic Security Systems

This chapter implements the lock and key control requirements of NPR 1620.3A.

7.1 General

7.1.1 Lock, key and electronic security systems requirements have been established at each GSFC site to protect areas, safeguard pilferable materials and supplies from unauthorized access, and prevent unauthorized disclosure of sensitive, restricted, or classified information.

7.1.2 All areas and materials that require protection as described above shall be secured through the application of security measures such as locking mechanisms, electronic security systems, or other "industry standard" locking devices.

7.1.3 Keys, access levels applied to PIV badges and keycards shall be issued only to authorized individuals who require access to the controlled areas. Keys and combinations to locking mechanisms shall be limited to the minimum number of individuals necessary.

7.2 Responsibilities

7.2.1 In addition to the responsibilities identified in NPR 1620.3A, the following additional responsibilities are identified for key, lock, and electronic security systems.

7.2.2 GPSD shall be responsible for establishing and maintaining the program for keys, locks, and electronic access controls and ensuring uniform implementation throughout GSFC.

7.2.3 Supervisors shall be responsible for approvals and ensuring that only authorized personnel are issued access control devices, e.g., keys, access levels applied to PIV badges and keycards.

7.3 Key and Lock Systems

7.3.1 GSFC Key and Lock System consist of two components:

a. Limited Access Security System (LASS) – Used to protect special areas and functions designated by GPSD. Keys to areas protected by a LASS are absolutely restricted to the individual user(s) and GPSD staff.
b. Building System – Used to protect general offices, suites, laboratories, and areas not designated or protected under a LASS. Keys to areas protected by the Building System are issued to those needing access in the course of their daily duties and only to the level required for the conduct of their assigned responsibilities.

7.3.1.1 Only locking mechanisms approved by GPSD will be authorized for these purposes. The number of individuals authorized to receive or retain keys and lock combinations shall be kept to the minimum necessary.

7.3.2 Master Keys

7.3.2.1 Master Keys shall be strictly controlled. Master Keys include Building Grand Masters, Building Sub-Masters, Area and Suite Masters, LASS Masters, and Special Area Masters. The following apply at Greenbelt and WFF, but not at IV&V or GISS.

a. Building Grand Masters – Building grand master keys shall be issued only to personnel with a

direct need for Center-wide access in the performance of official duties. Requests for issuance shall come from the appropriate directorate through the Director of Management Operations to GPSD, and shall include a complete justification of the need.

b. Building Sub-Masters – Sub-masters are for individual buildings and will be issued to the respective FOM once approved by the FOM Chairman. Other persons requiring sub-masters in the performance of official duties shall forward a written request, through the appropriate directorate and FOM, to the CCPS for approval. The request shall include a complete justification of the need for the key.

c. Area and Suite Masters – Requests for these keys shall be submitted to GPSD through the appropriate division chief or branch head responsible for the suite or area.

d. LASS Masters – LASS masters shall be issued only to security personnel with approval of the CCPS.

e. Special Area Masters – Janitorial storage areas and mechanical or electrical equipment room keys shall be requested through the Chief, Facilities Management Division (FMD). Telephone closet keys shall be requested through the Information Technology and Communications Directorate.

7.3.3 Obtaining Keys and Locks

a. Acquisition – GPSD controls locks, security containers (i.e., safes), combinations, and keys. All requests for the purchase of locks, locking devices, locking security containers (i.e., safes), electronic security controls, alarms, etc., through small purchases, store stock purchases, or "mass" purchases, require approval by GPSD to ensure compatibility with existing control systems and locking procedures.
   1) Padlocks and Keys – All requests to purchase padlocks and keys require approval by GPSD. Equipment and materials shall be secured in accordance with NPR 1620.3A. Individuals responsible for areas with a need for padlocks and keys shall contact GPSD for more specific guidelines and requirements.
   2) Cipher Locks – Cipher locks are not generally used at GSFC. However, GPSD may approve the use of cipher locks for areas or rooms with special security needs, or which meet unique security circumstances and cannot feasibly be secured in any other manner. Individuals responsible for areas with a need for a cipher lock shall contact GPSD for more specific guidelines and requirements.

b. Issuance – Keys, access levels applied on PIV badges and proximity keycards shall be issued only to authorized individuals with a valid need for access into a room, facility, or area. All locks, keys, keycards, locking devices, and other such items intended to control access on the Center or its facilities shall be issued through GPSD. Requests for keys, access levels applied to PIV badges or keycards shall be made using the eMOD request system at GSFC and routed through the appropriate branch head or approving official to GPSD key control office. After the key control

office verifies the information, the key control office will notify the requestor(s) that the key(s) or keycard(s) is (are) ready for pick up, or NASA PIV card has been updated.

1) At WFF, GSFC 24-12 or 24-12A shall be routed to the WFF Security Office through the appropriate FOM, Facility Security Manager, or other approving official. In order to receive a key or keycard at WFF, personnel must have a NASA or GSFC Center specific badge.
2) IV&V and GISS will develop their own procedures, and provide a copy of those procedures to the GPSD.

c. Installation or Replacement – All requests for the installation or replacement of locks, locking devices, or access control systems (whether for new construction, renovations, or other reasons) at GSFC shall be processed through GPSD using eMOD. GPSD shall verify compatibility with existing control systems and locking procedures.

1) Desks and File Cabinets: GPSD will provide replacement locks and keys for desks, file cabinets, and other similar containers on a limited basis, as available.
2) Doors: GPSD will provide or replace locks and keys for doors as available on rooms or areas requiring access controls, except for new construction or renovations contracted through FMD, for which GPSD will only provide keys.
3) Repair of Defective Locks/Knobs: GPSD coordinates locksmith repairs of defective locks and knobs.

7.3.4 Electronic Security Systems

Several types of electronic security systems are used on GSFC. These systems are monitored at Greenbelt by GPSD on a 24-hour basis to protect classified information or material, IT resources, Mission Control Centers, valuable property, or other sensitive areas requiring controlled and/or monitored access. At WFF, they are similarly monitored by the Emergency Operations Center. These systems are available through GPSD to all GSFC organizations with security needs requiring this level of protection.

a. Reports of access requested by organizations for areas under their control will be reviewed and approved by GPSD prior to being released to the requesting organization.

b. Specific questions regarding alarms and activations should be directed to GPSD.

7.3.5 Installation and Maintenance of Security Systems

All installations and repairs of security systems shall be requested through GPSD using eMOD request system. GPSD will determine if the system is required and coordinate authorized installation and maintenance of the equipment. Such systems shall comply with the National Fire Protection Association Code and the International Building Code.

7.3.6 Security of Locking Mechanisms

a. All controlled keys, access levels applied to PIV badges and keycards shall be requested using

GSFC eMOD request system. No markings or special codes will be placed on GSFC keys by users or others, except as issued by GPSD. Keys, keycards, and locking mechanisms may be transferred or duplicated only by GPSD. Keys which are no longer needed or no longer in use shall be returned to GPSD immediately upon removal of need or use. Access levels applied to PIV badges shall be deleted immediately upon removal of need for use.

b. Padlocks shall not be left in an open position while on a hasp or in storage. Padlocks shall be relocked after opening to prevent lock substitution.

7.3.7 Reporting Loss/Theft of Keys, PIV Badges and Keycards

7.3.7.1 Employees and contractors shall be responsible for protecting keys, PIV badges, keycards, and locks entrusted to them from damage, loss, or theft. When keys, keycards, and/or locks are discovered missing as a result of theft, negligence, or other loss, the missing item shall be reported immediately to GPSD.

7.3.7.2 The reporting individual shall then complete a Lost/Missing/Stolen Property Report (GSFC Form 24-10D). The individual shall obtain authorization for replacement on GSFC Form 24-10D and submit it to GPSD. The authorizing official for civil servants is the appropriate division chief or the authorizing official of the location or facility they are assigned to, and for contractors it is the contracting officer's technical representative.

7.3.7.3 There may be a waiting period before keycard or PIV replacement to allow for possible return by mail.

7.3.8 Requesting Security Work

Security work (e.g., lock and alarm installations, rekeying, lock and safe repairs, keycard installations, or other security work) shall be requested utilizing eMOD at GSFC. Inquiries regarding specific requirements for completing security work requests shall be directed to GPSD.

7.3.9 Locking Security Containers

GPSD shall be responsible for the accountability, placement, and maintenance of all locking security containers, safes, vaults, media storage containers, and areas or doors secured with combination locks. All requests for locking security containers for the storage of classified or sensitive material, the movement or placement of containers, maintenance of or combination changes for containers or locks, or procurements of locking security containers shall be coordinated with and approved by GPSD. GPSD can, on a limited basis, provide a locking heavy-duty security container or vault with a three-position dial combination lock approved for the storage of classified material. When this type of container is used for storage of classified material, the combination shall be changed at least annually.

Appendix A - Definitions

A.1 Access – The ability, opportunity, and authority to gain knowledge of information or gain authorized entry onto a NASA property, leased facilities, and IT resources.

A.2 Arrest – Seizure of the person based on probable cause that he/she has committed a felony or a misdemeanor in the presence of the officer. Subjecting the person to the will and control of the officer; circumstances that would lead a reasonable person to believe that he/she was not free to leave the presence of the officer. Brief detention for purposes of ascertaining a person's identity and/or activities, without more, is not an arrest.

A.3 Arrest Authority – The power to execute arrests, without a warrant, and to conduct searches incident to an arrest, granted to designated NASA security officials and security services contractors, as defined in 14 C.F.R. Part 1203b.

A.4 Asset – A system, object, person, or any combination thereof, that has importance or value; includes contracts, facilities, property, records, unobligated or unexpended balances of appropriations, and other funds or resources.

A.5 Center Chief of Protective Services/Center Chief of Security (CCPS/CCS) – The senior Center security official responsible for technical management and day-to-day operations of the Center's security program.

A.6 Certification – A formal process used by the certifying official to ensure that an individual has met all established training requirements as necessary to perform their security responsibilities.

A.7 Certifying Authority (CA) – Individual responsible for ensuring and certifying to the Designated Approving Authority, that requisite security measures are implemented for IT systems identified for processing of classified information.

A.8 Certifying Officials – The AA, OPS or the CCPS when so delegated, who are, by virtue of this NPR, authorized to certify that an individual has met established requirements (training, firearms qualification), can perform those security functions designated in their position description, and can carry a firearm in performance of their security duties. They can also approve the use of a security room, vault, or container for storage of CNSI.

A9. Classification Category – The specific degree of security classification that has been assigned to CNSI to indicate the extent of protection required in the national interest.

A.10 Classified information – Information that has been determined pursuant to Executive Order (EO) 13526, or a successor or predecessor order, or the Atomic energy Act of 1954 (42 U.S.C. 2011 et seq.) to require protection against unauthorized disclosure.

A.11 Contractor – An expert or consultant (not appointed under Section 5 USC § 3109) to an agency; an industrial or commercial contractor, licensee, certificate holder, or grantee of any agency, including all subcontractors; a personal services contractor; or any other category of person who performs work for or on behalf of NASA (but not a Federal employee).

A.12 Counterintelligence (CI) – Information gathered and activities conducted to protect against espionage and sabotage and other intelligence activities conducted for or on behalf of foreign powers, organizations, or persons or international terrorist activities, but not including personnel, physical, document, or communications security.

A.13 Critical Infrastructure – Systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters. (Public Law 107-56, U.S. Patriot Act Section 1016 (e))

A.14 Director, Security Management Division (DSMD) – Official assigned to OPS responsible for Agency management of physical security, personnel security, industrial security, and program security.

A.15 Electronic Access Control System – Electromechanical and electronic devices that monitor and permit or deny entry and exit of a protected area by personnel or vehicles.

A.16 Electronic Control Device (ECD) – Designed to disrupt a subject's central nervous system by means of deploying battery-powered electrical energy sufficient to cause uncontrolled muscle contractions and interrupt an individual's voluntary motor responses.

A.17 Executive Order (EO) – Official documents, numbered consecutively, through which the President of the United States manages the operations of the Federal Government.

A.18 Federal Arrest Authority (FAA) – The arrest authority granted under 14 C.F.R., Section 1203b.103 to NASA security personnel.

A.19 NASA Critical Infrastructure (NCI) – Key resources/assets that the Agency depends upon to perform and maintain its most essential missions and operations.

A.20 NASA Employees – NASA civil service personnel.

A.21 NASA PIV Badge – Refers to the NASA Photo-ID that has any number of embedded and external technologies capable of activating any type of facility, IT, or personal recognition access control system. Technology shall include: Exterior bar code and magnetic stripe embedded proximity chip, and embedded "smart card" chip.

A.22 NASA Policy Directive (NPD) – NPDs are policy statements that describe what is required by NASA management to achieve NASA's vision, mission, and external mandates and who is responsible for carrying out those requirements.

A.23 NASA Procedural Requirements (NPR) – NPRs provide Agency requirements to implement NASA policy as delineated in an associated NPD.

A.24 Risk Acceptance – An official acknowledgement by a management official that they accept the risk posed by not implementing a recommendation or requirement, designed to reduce or mitigate the risk.

A.25 Risk Assessment (RA) – The process of identifying internal and external threats and security vulnerabilities, identifying the likelihood of an event arising from the combination of such threats and vulnerabilities. Further, the RA defines the critical security countermeasures necessary to continue an organization's operations, defines the controls in place or necessary to reduce risk, and evaluates the cost for such controls.

A.26 Risk Management – A means whereby NASA management implements select measures designed to reduce or mitigate known risks.

A.27 Security Officer (SO) – An armed officer, who has successfully completed the required NASA training, but who is not to exercise NASA arrest authority, whose duties may include but are not limited to: first response to emergencies, mobile patrols, temporarily detain or seize with reasonable suspicion, inspections, perimeter and internal access control, contingency posts, and crowd control. An SO may request an SPO effect an arrest when he either has directly observed any Federal offense or has reasonable grounds to believe that a felony has been committed.

A.28 Security Police Officer (SPO) – An armed officer, who has successfully completed the required NASA training, with NASA Federal arrest authority, whose duties may include, but are not limited to,: first response to emergencies, enforces Federal law, mobile patrols, inspections and searches, traffic enforcement, investigations, and other duties as required. An SPO may affect an arrest on request of an SO, as stated above.

A.29 Security Specialist – A qualified and trained NASA civil service employee assigned to perform certain security duties such as physical, personnel, and program security functions.

A.30 Security Violation – An act or action by an individual or individual(s) that is in conflict with NASA security policy or procedure (including the loss or compromise of CNSI; refusal to properly display NASA Photo-ID; violation of escort policy; and security area violations). (NOTE: Does not include incidents of criminal activity, such as theft, assault, or driving under the influence).

A.31 Special Access Program (SAP) – Any program established and approved under (EO) 13526 that imposes need-to-know or access controls beyond those normally required for access to collateral Confidential, Secret, or Top Secret information.

A.32 Special Agent – A qualified and credentialed NASA civil service employee assigned to perform specialized security, investigative, or law enforcement duties authorized by statute and this NPR.

A.33 Threat Assessment – A formal, in-depth review and evaluation of the capabilities and interests of identified aggressors for the purpose of determining their potential for targeting NASA operations and assets. Used in conjunction with a Vulnerability Assessment to prepare an RA.

A.34 Unauthorized disclosure EO) 13526) – A communication or physical transfer of classified information to a recipient who does not have the appropriate credentials for access or may also be the result of inadvertent disclosure.

A.35 Waiver – The approved request for a permanent or extended exemption (more than 1 year) for compliance with a specific procedural requirement granted by the AA, Mission Support Directorate.

Appendix B- Acronyms

AA	Assistant Administrator
AA&E	Accountability of Arms, Ammunition, and Explosives
B&C	Badges and Credentials
CCPS	Center Chief of Protective Services
CCS	Chief of Security
CI	Counterintelligence
CNSI	Classified National Security Information
CT	Counterterrorism
DHS	Department of Homeland Security
DoD	Department of Defense
DNI	Director National Intelligence
DSMD	Director of Security Management Division
EMOD	Electronic Management Operations Directorate
EO	Executive Order
EOD	Ordinance Detection
EPACS	Electronic Physical Access Control System
FAA	Federal Arrest Authority
FMD	Facilities Management Division
FN	Foreign National
FOIA	Freedom of Information Act
FOM	Facility Operations Manager
GEWA	Government Employees Welfare Association
GISS	Goddard Institute for Space Studies
GPR	Goddard Procedural Requirements
GPSD	GSFC Protective Services Division, including security components at WFF, IV&V, and GISS
GSA	General Services Administration
GSFC	Goddard Space Flight Center, including WFF, IV&V, WSC and GISS
HAZMAT	Hazardous Materials
HSAS	Homeland Security Advisory System
ICD	Intelligence Community Directive
ID	Identification
IT	Information Technology
IVC	International Visit Coordinator
IV&V	Independent Verification and Validation Facility
LASS	Limited Access Security System
LISTS	Locator and Information Services Tracking System
MOU	Memorandum of Understanding
NASA	National Aeronautics and Space Administration
NCI	NASA Critical Infrastructure

NCIPP	NASA Critical Infrastructure Protection Program
NPD	NASA Policy Directives
NPR	NASA Procedural Requirements
NPSTA	NASA Protective Services Training Academy
NTAS	National Terrorism Advisory System
OC	Oleoresin Capsicum
OCC	Office of Communications
OGC	Office of the General Counsel
OIG	Office of the Inspector General
OIIR	Office of International and Interagency Relations
OPS	Office of Protective Services
OPSEC	Operations Security
PSD	Protective Services Division
PIV	Personal Identity Verification
PPD	Presidential Policy Directive
RA	Risk Assessment
RAA	Risk Acceptance Authority
RVI	Random Vehicle Inspection
SA	Special Agent
SAP	Special Access Program
SAPSG	Special Access Program Security Guide
SATERN	System for Administration, Training, and Educational Resources for NASA (SATERN)
SCI	Sensitive Compartmented Information
SF	Standard Form
SETA	Security Education, Training, and Awareness
SO	Security Officer
SPO	Security Police Officer
USPP	U.S. Park Police
UVA	University of West Virginia
WIIMS	Wallops Institutional Information Management System
WFF	Wallops Flight Facility

Appendix C - Espionage and Terrorism Indicators

An increasing number of studies and reports have indicated that specific behaviors or characteristics are frequently exhibited by individuals engaged in espionage and/or terrorist activities. Some of these reports are:

DHS, "Report Suspicious Behavior and Activity"
http://www.us-cert.gov/sites/default/files/publications/PYWReportSuspiciousBehavior.pdf

DOJ/FBI, "Preventing Terrorist Attacks – How You Can Help"
http://www.fbi.gov/about-us/investigate/terrorism/help-prevent-terrorist-attacks

DOJ/FBI, "Intellectual Property Protection"
http://www.fbi.gov/about-us/investigate/counterintelligence/intellectual_property_protection

DOJ/FBI, "Visitors: Risks and Mitigations"
http://www.fbi.gov/about-us/investigate/counterintelligence/Risks%20-%20Mitigations%20of%20Visitors%20Brochure.pdf

DOJ/FBI, "The Insider Threat"
http://www.fbi.gov/about-us/investigate/counterintelligence/insider_threat_brochure

DOJ/FBI, "Elicitation"
http://www.fbi.gov/about-us/investigate/counterintelligence/elicitation-brochure

The following lists of indicators have been developed:

Espionage Indicators

While common features abound, it is important to note that these factors are descriptive and not predictive. That is, certain behaviors and personality characteristics have been found to be associated with persons who have engaged in espionage, but they are by no means exclusive to that set of people. The important lesson here is that managers and coworkers should be sensitive to the following types of indicators, and report behaviors that suggest possible espionage activity.

a. Removing classified or sensitive information from the workplace without authorization.
b. Visiting foreign diplomatic establishments in the United States or abroad without any logical reason or permission.
c. Maintaining close associations with officials from designated countries.
d. Engaging in personal business dealings/private ventures with individuals from foreign governments or corporations.
e. Maintaining bank accounts in foreign countries.
f. Frequently working alone and after scheduled work hours without any logical reason or explanation.

g. Unauthorized/unexplained continuous contact with foreign governments or foreign corporations.
h. Violating or circumventing established security practices.
i. Frequent security violations.
j. Exhibiting undue curiosity in projects/programs without logical explanation or "need-to-know." Loitering in areas where sensitive/classified projects are being conducted when the individual is not involved in the project.
k. Displaying a reluctance to submit paperwork for a security clearance when requested/needed for work.
l. Exhibiting signs of having more money/valuables than salary or family circumstances would allow.
m. Experiencing a sudden unexplained reversal of a financial situation.
n. Bringing unauthorized/unexplained cameras, recording devices, or other similar unauthorized equipment into work areas.
o. Attempting to entice other employees or contractors into questionable/illegal activities.
p. Expressing disaffection with NASA programs/projects/employees/contractors and seeking to get revenge.
q. Demonstrating unusual travel patterns such as last-minute personal trips of short duration and attempting to conceal trips from supervisors/co-workers.
r. Attempting to gain unauthorized access to computer systems/networks.

Terrorism Indicators:

Prior to every terrorist attack, someone has to "check out" the target to gather needed intelligence. This action is normally performed through: Surveillance; Elicitation; Theft; Tests of Security; and Rehearsals. You should report the following:

a. Sketching, mapping, photographing, or conducting surveillance of GSFC facilities.
b. Suspicious persons or vehicles.
c. Individuals asking suspicious questions about GSFC facilities, activities or personnel.
d. Unauthorized individuals attempting to gain access to GSFC facilities.
e. Theft of or attempts to obtain security uniforms, identification cards, or equipment.
f. Lost or stolen official identification which could be used or altered to gain access to GSFC.
g. Stolen official government vehicles, which may be used to access GSFC facilities.
h. Lost, stolen or any suspicious attempts to obtain blueprints, floor plans, alarm schematics, detailed maps, or other information which could be used to plan a terrorist attack.
i. Any discovery of documents, particularly in foreign languages, which appear to contain pictures or drawings of GSFC facilities or other key infrastructure.
j. Information overheard about any planned international or domestic terrorist activity.
k. Incidents where terrorist organizations offer employment or training to US persons or ask for assistance in the design, manufacture, maintenance, or employment of terrorist weapons.

CHANGE HISTORY LOG

Revision	Effective Date	Description of Changes
Baseline	04/03/08	Initial Release
A	02/21/14	Removal of requirements and information within the document GPR 1600.1 associated with Personnel Security, Classified National Security Information, and Credential Management. These requirement and information have been included in new GPRs, GPR 1600.2, GPR 1600.3 and GPR 1600.4 respectively, to align with the approved corresponding NPRs. In addition, information regarding physical security, training and use of force by the security officers providing services at GSFC requirements has been updated and included. These new requirements align with requirements identified within NPR 1600.1A.